

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

**IN RE: BPS DIRECT, LLC and
CABELA’S, LLC, WIRETAPPING**

**MDL NO. 3074
2:23-md-03074-MAK**

DEFENDANTS’ REPLY IN SUPPORT OF THEIR MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

I. Plaintiffs Lack Article III Standing..... 2

II. Plaintiffs’ Wiretap Claims Fail 8

III. Plaintiffs’ Invasion of Privacy Claims Fail..... 14

IV. Plaintiffs’ CFAA Claim Fails. 16

V. Plaintiffs’ Unfair Competition Claims Fail..... 17

VI. Plaintiffs’ Conversion, Trespass, and Larceny Claims Fail..... 18

CONCLUSION..... 19

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Adams v. PSP Grp., LLC</i> , 2023 WL 5951784 (E.D. Mo. Sept. 13, 2023).....	<i>passim</i>
<i>Bohnak v. Marsh & McLennan Companies, Inc.</i> , 79 F.4th 276 (2d Cir. 2023)	5
<i>Bowen v. Porsche Cars, N.A., Inc.</i> , 561 F. Supp. 3d 1362 (N.D. Ga. 2021)	16
<i>Brignola v. Home Properties, L.P.</i> , 2013 WL 1795336 (E.D. Pa. Apr. 26, 2013)	8
<i>Brown v. Google LLC</i> , 2023 WL 5029899 (N.D. Cal. Aug. 7, 2023)	3
<i>Bunnell v. MPAA</i> , 567 F.Supp.2d 1148 (C.D. Cal. 2007)	9
<i>Byars v. Sterling Jewelers, Inc.</i> , 2023 WL 2996686 (C.D. Cal. Apr. 5, 2023)	4
<i>Calhoun v. Google LLC</i> , 526 F. Supp. 3d 605 (N.D. Cal. 2021)	6, 17
<i>Cardoso v. Whirlpool Corp.</i> , 2021 WL 2820822 (S.D. Fla. July 6, 2021).....	10
<i>Commonwealth v. Byrd</i> , 235 A.3d 311 (Pa. 2020)	13
<i>Commonwealth v. Proetto</i> , 771 A.2d 823 (Pa. Super. Ct. 2001), <i>aff'd</i> , 837 A.2d 1163 (Pa. 2003).....	13
<i>Cook v. Gamestop, Inc.</i> , 2023 WL 5529772 (W.D. Pa. Aug. 28, 2023)	<i>passim</i>
<i>Dickson v. Direct Energy, LP</i> , 69 F.4th 338 (6th Cir. 2023)	3
<i>In re DoubleClick Inc. Priv. Litig.</i> , 154 F. Supp. 2d 497 (S.D.N.Y. 2001).....	9

<i>Drazen v. Pinto</i> , 74 F.4th 1336 (11th Cir. 2023)	3
<i>Eagle v. Morgan</i> , 2011 WL 6739448 (E.D. Pa. Dec. 22, 2011)	16
<i>Eichenberger v. ESPN, Inc.</i> , 876 F.3d 979 (9th Cir. 2017)	3
<i>In re Facebook, Inc. Internet Tracking Litig.</i> , 956 F.3d 589 (9th Cir. 2020)	3
<i>Freeman Health System v. Wass</i> , 124 S.W.3d 504 (Mo. Ct. App. 2004)	17, 18
<i>Goldstein v. Costco Wholesale Corp.</i> , 559 F. Supp. 3d 1318 (S.D. Fla. 2021)	10, 12
<i>In re Google Inc.</i> , 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013)	13
<i>Greenley v. Kochava, Inc.</i> , 2023 WL 4833466 (S.D. Cal. July 27, 2023)	4
<i>Hazel v. Prudential Fin., Inc.</i> , 2023 WL 3933073 (N.D. Cal. June 9, 2023)	6
<i>Jacome v. Spirit Airlines, Inc.</i> , 2021 WL 3087860 (Fla. Cir. Ct. June 17, 2021)	10, 12
<i>Jones v. Bloomingdales.com, LLC</i> , 2023 WL 6064845 (E.D. Mo. Sept. 18, 2023)	3, 5, 6, 8
<i>Katz-Lacabe v. Oracle Am., Inc.</i> , 2023 WL 2838118 (N.D. Cal. Apr. 6, 2023)	17
<i>Krakauer v. Dish Network, LLC</i> , 925 F.3d 643 (4th Cir. 2019)	3
<i>Kurowski v. Rush Sys. for Health</i> , 2023 WL 2349606 (N.D. Ill. Mar. 3, 2023)	15
<i>Lightoller v. Jetblue Airways Corp.</i> , 2023 WL 3963823 (S.D. Cal. June 12, 2023)	6
<i>Lupia v. Medicredit, Inc.</i> , 8 F.4th 1184 (10th Cir. 2021)	3

<i>Massie v. Gen. Motors LLC</i> , 2022 WL 534468 (D. Del. Feb. 17, 2022)	<i>passim</i>
<i>Mikulsky v. Noom, Inc.</i> , 2023 WL 4567096 (S.D. Cal. July 17, 2023)	3, 8
<i>Moore v. Centrelake Med. Grp., Inc.</i> , 299 Cal. Rptr. 3d 544 (Cal. Ct. App. 2022)	17
<i>In re Nickelodeon Cons. Priv. Litig.</i> , 827 F.3d 262 (3d Cir. 2016)	6, 16
<i>Norris v. Norris</i> , 731 S.W.2d 844 (Mo. 1987)	18
<i>O'Donnell v. United States</i> , 891 F.2d 1079 (3d Cir. 1989)	15
<i>Perez v. McCreary, Veselka, Bragg & Allen, P.C.</i> , 45 F.4th 816 (5th Cir. 2022)	3
<i>Persinger v. Sw. Credit Sys., L.P.</i> , 20 F.4th 1184 (7th Cir. 2021)	3
<i>Revitch v. New Moosejaw, LLC</i> , 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019)	12
<i>Rodriguez v. Google LLC</i> , 2021 WL 2026726 (N.D. Cal. May 21, 2021)	10
<i>Saleh v. Nike, Inc.</i> , 562 F. Supp. 3d 503, 518 (C.D. Cal. 2021)	10
<i>Schmerling v. Injured Workers' Ins. Fund</i> , 795 A.2d 715 (Md. 2002)	12
<i>Smith v. Facebook, Inc.</i> , 262 F.Supp.3d 943 (N.D. Cal. 2017), <i>aff'd</i> 745 F. App'x 8 (9th Cir. 2018)	9
<i>Spokeo, Inc. v. Robins</i> , 578 U.S. 330 (2016)	3
<i>Straubmuller v. Jetblue Airways Corp.</i> , 2023 WL 5671615 (D. Md. Sept. 1, 2023)	3, 6, 7, 8
<i>Susinno v. Work Out World Inc.</i> , 862 F.3d 346 (3d Cir. 2017)	3

TransUnion v. Ramirez,
141 S. Ct. 2190 (2021).....2, 3, 4, 5

United States v Soybel,
13 F.4th 584 (7th Cir. 2021)16

Van Buren v. United States,
141 S. Ct. 1648 (2021).....16

Weicht v. Suburban Newspapers of Greater St. Louis, Inc.,
32 S.W.3d 592 (Mo. App. 2000)18

Yoon v. Lululemon USA, Inc.,
549 F. Supp. 3d 1082-83 (C.D. Cal. 2021)10

Statutes

Cal. Pen. Code § 631(a)9

Other Authorities

Fed. R. Civ. P. 9(b)2, 19

Plaintiffs' Opposition to Defendants' Motion to Dismiss, ECF No. 56 ("Opposition" or "Opp."), makes clear that this case should begin and end with the threshold issue of standing (Section I *infra*). Faced with an unbroken string of federal courts dismissing virtually identical claims for lack of standing, Plaintiffs regurgitate arguments that were directly rejected by those courts over and over again. Plaintiffs' allegations that Defendants used session replay code to capture data about Plaintiffs' interactions with Defendants' websites simply do not give rise to the type of injury that would allow them to bring their claims in federal court. This Court should join its sister courts in dismissing these types of claims.

But even if Plaintiffs did have standing to bring their claims, each of those claims still fails for a number of reasons, each of which is addressed at length in Defendants' Memorandum In Support of Their Motion to Dismiss, ECF No. 54-1 ("Motion" or "Mot."). Plaintiffs' Opposition does not effectively combat any of those arguments.

As to Plaintiffs' claims under various state and federal wiretap statutes (Section II *infra*), Plaintiffs fail to allege at least one essential element of each of their claims. *See* ECF No. 54-2. Moreover, Defendants' use of technology like session replay code to analyze interactions with their websites was clearly disclosed in Defendants' Privacy Notices, which is sufficient to establish Plaintiffs' consent.

Plaintiffs' various invasion of privacy claims (Section III *infra*) fare no better. Plaintiffs fail to allege the requisite intent for the intentional tort of invasion of privacy. Plaintiffs also have no reasonable expectation of privacy in any of the innocuous data that they allege is collected here. Finally, Plaintiffs fail to allege that Defendants engaged in any "highly offensive" behavior that could give rise to an invasion of privacy claim.

Plaintiffs’ claim under the Computer Fraud and Abuse Act (“CFAA”) fails also (Section IV *infra*). Plaintiffs fail to allege any unauthorized “access” to their devices, and fail to allege an ascertainable “loss” under the statute.

Certain Plaintiffs’ claims under the California Unfair Competition Law (“UCL”) and Missouri Merchandising Practices Act (“MMPA”) (Section V *infra*) each fail for separate reasons. Plaintiffs cannot support a UCL claim because they lack statutory standing to bring claims under that statute. The MMPA claim fails because Plaintiffs do not allege a “purchase” of any merchandise or service, do not allege a causal connection between Defendants’ supposed fraud and any “merchandise,” and do not allege an ascertainable loss under the statute.

Finally, Plaintiffs claims for conversion, trespass, and larceny (Section VI *infra*) all fail. Plaintiffs cannot state a claim for conversion or trespass because they do not show a physical intermeddling. Similarly Plaintiffs cannot state a statutory larceny claim under California law because they fail to allege the claim with particularity, as required by Fed. R. Civ. P. 9(b), do not allege the requisite intent, and do not allege the type of loss required by the statute.

I. Plaintiffs Lack Article III Standing.

“Only those plaintiffs who have been *concretely harmed* by a defendant’s statutory violation may sue that private defendant over that violation in federal court.” *TransUnion v. Ramirez*, 141 S. Ct. 2190, 2204 (2021). Plaintiffs’ opposition to Defendants’ standing argument is fundamentally flawed and makes clear that Plaintiffs do not to have alleged the necessary concrete injury to bring their claims in this Court.

Plaintiffs rely on authority that pre-dates the Supreme Court’s clarification in *TransUnion*, of Article III standing requirements in cases where Plaintiffs allege statutory violations. A cascade of courts across the country addressing Article III in the specific context at issue here—the alleged use of session replay technology to capture website interactions—have time and again dismissed

these cases for lack of standing. *See, e.g., Jones v. Bloomingdales.com, LLC*, 2023 WL 6064845 (E.D. Mo. Sept. 18, 2023); *Adams v. PSP Grp., LLC*, 2023 WL 5951784 (E.D. Mo. Sept. 13, 2023); *Straubmuller v. Jetblue Airways Corp.*, 2023 WL 5671615 (D. Md. Sept. 1, 2023); *Cook v. Gamestop, Inc.*, 2023 WL 5529772 (W.D. Pa. Aug. 28, 2023); *Mikulsky v. Noom, Inc.*, 2023 WL 4567096 (S.D. Cal. July 17, 2023); *Massie v. Gen. Motors LLC*, 2022 WL 534468 (D. Del. Feb. 17, 2022). Plaintiffs do not meaningfully try to distinguish this case from those cases in any way, instead simply asserting, without explanation, that those cases applied an “improperly broad” interpretation of *TransUnion* before going on to discuss the ruling in *Spokeo, Inc. v. Robins*, 578 U.S. 330 (2016)—not *TransUnion*. Opp. at 7-8. Plaintiffs do not cite a single, post-*TransUnion* case analyzing claims based on session replay technology where a court found Article III standing.¹

This is not surprising. The opinions in the cases cited by Defendants are well-reasoned in rejecting the precise arguments Plaintiffs raise here. In short, Plaintiffs claim that, because wiretapping can give rise to a common law cause of action, standing in a wiretap case depends on whether a wiretap is alleged.² Opp. at 4-6. But this circular line of reasoning was explored and

¹ In Footnote 3, Plaintiffs cite to a string of cases for the proposition that “so long as the underlying type of harm is similar, the quantity or extent of the harm need not be the same.” Opp. at 4 n.3. None of these cases require the court to find standing here. Each either analyzes a different type of harm, under a different statute, than those implicated by Plaintiffs here or predated *TransUnion*—or both. *See Drazen v. Pinto*, 74 F.4th 1336, 1339–40 (11th Cir. 2023) (analyzing standing under TCPA); *Dickson v. Direct Energy, LP*, 69 F.4th 338, 341 (6th Cir. 2023) (same); *Perez v. McCreary, Veselka, Bragg & Allen, P.C.*, 45 F.4th 816, 822–23 (5th Cir. 2022) (finding no standing for FDCPA claims under *TransUnion*); *Lupia v. Medicredit, Inc.*, 8 F.4th 1184, 1192 (10th Cir. 2021) (analyzing standing for FDCPA claims); *Persinger v. Sw. Credit Sys., L.P.*, 20 F.4th 1184, 1192 (7th Cir. 2021) (analyzing standing for FCRA claims); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020) (analyzing standing pre-*TransUnion*); *Krakauer v. Dish Network, LLC*, 925 F.3d 643, 653–54 (4th Cir. 2019) (discussing TCPA standing pre-*TransUnion*); *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 982–83 (9th Cir. 2017) (analyzing standing for VPPA violations pre-*TransUnion*); *Susinno v. Work Out World Inc.*, 862 F.3d 346, 351–52 (3d Cir. 2017) (analyzing TCPA standing pre-*TransUnion*).

² Even the cases that Plaintiffs cite do not adopt this position. *See Brown v. Google LLC*, 2023 WL 5029899 at *5-6 (N.D. Cal. Aug. 7, 2023) (recognizing that “the standing analysis is contextual”

rejected by the court in *Cook v. GameStop*. 2023 WL 5529772 at *3–4. There the court explained that allowing the standing inquiry to begin and end with the statutory violation “runs directly counter to the Supreme Court’s clarification that a legislature’s creation of a statutory prohibition or obligation and a cause of action does not relieve courts of their responsibility to independently decide whether a plaintiff has suffered a concrete harm under Article III. *Id.* at *3 (quoting *Lightoller v. Jetblue Airways Corp.*, 2023 WL 3963823 at *3 (S.D. Cal. June 12, 2023)); *see also* *Byars v. Sterling Jewelers, Inc.*, 2023 WL 2996686, at *3 (C.D. Cal. Apr. 5, 2023) (rejecting, with respect to chat message tracking claims, the contention that “any violation of CIPA necessarily constitutes an injury in fact without the need for an additional showing of harm” as conflicting with *TransUnion*).

The *Adams* court similarly rejected this argument when it found that session replay plaintiffs lacked standing. In that case, like here, the plaintiff argued that “wiretapping statutes are designed to protect privacy rights, therefore, an alleged violation of a wiretapping statute must involve a harm to privacy rights, which have been historically recognized as forming the basis for privacy torts.” *Adams*, 2023 WL 5951784 at *6. The *Adams* court, agreeing with the court in *Cook*, rejected this argument “as it would mean any alleged violation of a wiretap statute necessarily constitutes an injury in fact even without allegations of actual harm”—a proposition that *TransUnion* explicitly rejected. *Id.* (citing *TransUnion*, 141 S. Ct. at 2205).

Plaintiffs argue that the *Cook* and *Massie* courts (and by extension all of the other decisions that Defendants cite) incorrectly “required the privacy interests the plaintiffs alleged to *be identical*

and ultimately finding the allegations there sufficient “to confer standing *given the sensitivity of the evidence at issue.*” (emphasis added); *Greenley v. Kochava, Inc.*, 2023 WL 4833466 at *3 (S.D. Cal. July 27, 2023) (finding, with little analysis and cursory reference to *TransUnion*, allegations involving collection of geolocation data, among additional types of data, sufficient to confer standing).

to the right to privacy recognized at common law.” Opp. at 7. That is incorrect. Indeed, the *Cook* plaintiff—represented by some of the same Plaintiffs’ counsel here—made this exact same argument with respect to *Massie* in the *Cook* case. *Cook*, 2023 WL 5529772 at *5. The *Cook* court rejected the argument, looking at the actual opinion in *Massie* and saying, “the court there compared the conduct alleged to the analogous harms of invasion of privacy and an encroachment on the plaintiffs’ interest in controlling their personal information and found that there was not a close relationship between the two.” *Id.* The *Cook* court went on to make that same comparison,³ which “is precisely what the Supreme Court instructed lower courts to do in *TransUnion*.” *Id.* The only thing that is different now from when the *Cook* plaintiff advanced Plaintiffs’ arguments is that a continuously growing number of courts have joined the *Massie* court in rejecting Plaintiffs’ argument. *See, e.g., Jones*, 2023 WL 6064845 at *1; *Adams*, 2023 WL 5951784 at *6; *Cook*, 2023 WL 5529772 at *5. This Court should follow suit.

Plaintiffs’ cite pre-*TransUnion* Third Circuit cases do not require a different outcome here. *See* Opp. at 6 (citing *In re Google Inc. Cookie Placement Cons. Priv. Litig.*, 934 F.3d 316, 325 (3d Cir. 2019); *In re Nickelodeon Cons. Priv. Litig.*, 827 F.3d 262, 271 (3d Cir. 2016)). These are the same cases that the *Cook* plaintiff relied on to advance her standing argument. *See Cook*, 2023 WL 5529772 at *5. The *Cook* court noted that “[a] close look at those decisions reflects that they might

³ In *Cook*, the plaintiff argued that the defendant’s alleged wiretapping through the use of session replay technology was analogous to the common-law tort of public disclosure of private facts. *Cook*, 2023 WL 5529772 at *4. Plaintiffs here offhandedly make the same argument, in the alternative to their primary argument based on intrusion upon seclusion. Opp. at 3 n.2. This throwaway statement does not establish standing because: (1) this is the exact argument rejected by the *Cook* court; and (2) the *Bohnak v. Marsh & McLennan Companies, Inc.*, 79 F.4th 276 (2d Cir. 2023), case Plaintiffs cite in support says nothing about standing for claims like these. *Bohnak* dealt with a data breach implicating the plaintiff’s personal sensitive information, including “Social Security or other federal tax identification number[s],” which gave rise to Article III standing. *Id.* at 280.

be abrogated by *TransUnion*[,] [b]ut even if they weren't, they are distinguishable" and went on to distinguish the type of personal information at issue in those cases with the internet browsing activity at issue in session replay cases. *Id.* (internal citations omitted). The *Massie* court likewise distinguished *Nickelodeon* and *Google*, finding that neither case requires a court to find Article III standing in a session replay case like this one. *Massie*, 2022 WL 534468 at *3.⁴

Put simply, post-*TransUnion*, "a bare [statutory] violation by itself is insufficient to demonstrate Article III injury in fact." *Lightoller*, 2023 WL 3963823, at *3. Accordingly, to determine whether Plaintiffs have standing to bring their claims, the Court here must determine "whether Plaintiff[s] adequately allege facts showing a harm that is closely related to the harm that forms the basis of the tort of intrusion upon seclusion." *Adams*, 2023 WL 5951784 at *6. As every court to consider the question has decided, where, as here, Plaintiffs do not allege that they actually communicated any specific, personal private information with a defendant's website, the alleged collection of website interactions by session replay code "is not closely related to the harm upon which the tort of intrusion of seclusion is based—or any invasion of privacy tort for that matter." *Adams*, 2023 WL 5951784 at *7; *see also Jones*, 2023 WL 6064845 at *2; *Straubmuller*, 2023 WL 5671615 at *5; *Cook*, 2023 WL 5529772 at *4; *Massie*, 2022 WL 534468 at *3.

To the extent Plaintiffs' Opposition even addresses this question, it argues essentially two things: (1) that the session replay technology captured personal information in the form of "products they searched for or purchased" (Opp. at 8 (citing Compl. ¶¶ 38–52)); and (2) that "two Plaintiffs allege they made website purchases." Opp. at 8 (citing Compl. ¶¶ 104, 117).

⁴ Plaintiffs' string of cases cited in FN 4 were nearly all similarly decided pre-*TransUnion* and therefore similarly lack weight. The only post-*TransUnion* case cited in that footnote, *Hazel v. Prudential Fin., Inc.*, 2023 WL 3933073 (N.D. Cal. June 9, 2023) does not address Article III standing.

Plaintiffs’ first argument fails for at least two reasons. First, paragraphs 38-52 of the Complaint do not say *anything* about the information that was allegedly captured by the session replay code. Instead, these paragraphs—in a section titled “Article III Standing”—merely summarize Plaintiffs’ allegations that Defendants violated wiretap laws and that Plaintiffs have common law invasion of privacy claims.⁵ *See* Compl. ¶¶ 38–52. In other words, these allegations simply rehash Plaintiffs’ argument on standing that has been routinely rejected by courts, as discussed above.

Second, the fact that Plaintiffs Cornell and Montecalvo allege that they made purchases on Defendants’ websites does not save their claims. As an initial matter, the Complaint is devoid of any factual allegation that Defendants configured session replay code to capture any information on the payment pages of its websites. This reason alone is sufficient for the Court to find that Plaintiffs Cornell and Montecalvo also lack standing. *See, e.g., Straubmuller*, 2023 WL 5671615, at *4 (dismissing session replay claims for lack of standing because it is not enough to allege that “Session Replay Code *could* capture personal information” including “personally identifying information and credit card details”); *Cook*, 2023 WL 5529772 at *7 (finding allegations “about how Session Replay Code works ‘in general’” as being “problematic” because “notably absent are any specific allegations about whether [defendant’s] code operated in the manner described”).

But even if Plaintiffs had alleged that Defendants had session replay code configured on the payment portions of their website, Plaintiffs Cornell and Montecalvo still would not have standing because “name, address, phone number, etc. . . . are not private facts actionable for an

⁵ Plaintiffs also fail to explain how Plaintiff Durham can possibly have standing when the Complaint does not even contain the conclusory allegations about his alleged experience with the websites that are present for the other Plaintiffs in the portion of the Complaint titled “Plaintiffs’ and Class Members’ Experiences.” Mot. at 4 n.3; *see also* Compl. ¶¶ 97–136. The Opposition, much like the Complaint, says nothing about Plaintiff Durham’s alleged experiences.

[invasion of privacy] claim.” *Brignola v. Home Properties, L.P.*, 2013 WL 1795336, at *12 (E.D. Pa. Apr. 26, 2013). This is precisely the type of information that Plaintiffs Cornell and Montecalvo would have communicated with Defendants’ websites in order to complete their purchases. *See* Compl. ¶¶ 104 (“During [her purchase], Plaintiff Cornell communicated with BPS by, *inter alia*, telling BPS what product she was interested in, what color chair she wanted, and where she wanted the chair shipped (i.e., her address and other personal information).”), 117 (“During [his purchase], Plaintiff Montecalvo communicated with Cabela’s by, *inter alia*, telling Cabela’s what product he was interested in, what color belt he wanted, and where he wanted the belt shipped (i.e., his address and other personal information).”).⁶

In sum, the weight of authority is clear. Every post-*TransUnion* court to consider the standing of session replay plaintiffs—often with nearly identical allegations to those contained in the Complaint here and considering the same arguments that Plaintiffs raise in opposition here—has dismissed plaintiffs’ claims for lack of standing. *See Jones*, 2023 WL 6064845; *Adams*, 2023 WL 5951784; *Straubmuller*, 2023 WL 5671615; *Cook*, 2023 WL 5529772; *Mikulsky*, 2023 WL 4567096; *Massie*, 2022 WL 534468. Plaintiffs do not proffer any examples of courts finding otherwise in these types of cases, and they do not effectively distinguish those cases from the allegations they bring here. Plaintiffs do not allege an injury that gives rise to standing and their Complaint makes clear that this case should be dismissed.

II. Plaintiffs’ Wiretap Claims Fail

A. Defendants’ Party Status Defeats California, Missouri, and Federal Wiretap Claims.

⁶ To the extent the Court agrees that the mere allegation that Plaintiffs’ Cornell and Montecalvo made a purchase on Defendants’ websites is sufficient to establish their standing, Counts III, IV, V, VI, VII, X, XI, and XII must still be dismissed as those claims are not, and cannot be, brought by either Plaintiff Cornell or Plaintiff Montecalvo.

Plaintiffs do not—and cannot—contest the fact that Defendants are parties to any alleged communication at issue here. Instead, Plaintiffs argue that: (1) as to the California statute, Defendants can be held liable for “aiding” the alleged interception (Opp. at 10–11); and (2) that Plaintiffs adequately allege a tortious purpose under the Missouri and Federal statutes. Opp. at 11–13.

As to the California claim, as Plaintiffs concede, an aiding theory of liability under the portion of the California statute that Plaintiffs identify is only available when the contents of a message are intercepted “while the same is in transit.” Opp. at 10 (citing Cal. Pen. Code § 631(a)). But as explained in Defendants’ Motion, Plaintiffs fail to allege that any such contemporaneous interception occurred. Mot. at 14–15. Accordingly, as no contents of a communication were captured “in transit,” there can be no “aiding” liability under Section 631(a). *See Smith v. Facebook, Inc.*, 262 F.Supp.3d 943, 951 (N.D. Cal. 2017), *aff’d* 745 F. App’x 8 (9th Cir. 2018) (dismissing CIPA wiretap claim because the connection with and transmission to Facebook due to pixels, web beacons, cookies, and code instructions happens independently); *Bunnell v. MPAA*, 567 F.Supp.2d 1148, 1153–54 (C.D. Cal. 2007) (forwarding duplicate copies of communications, even within milliseconds, was not an interception in transit).

As to the claims under the Missouri and federal statutes, Plaintiffs’ Opposition completely ignores the litany of cases cited in Defendants’ Motion demonstrating that a plaintiff cannot allege a tortious purpose merely by alleging that a tort was ultimately committed. Mot. at 9–10 (*citing, e.g., In re DoubleClick Inc. Priv. Litig.*, 154 F. Supp. 2d 497, 515 (S.D.N.Y. 2001) (the “criminal or tortious” requirement “cover[s] only acts accompanied by a specific contemporary intention to commit a crime or tort”). The Complaint alleges—and Plaintiffs reassert in their Opposition—that Defendants’ alleged purpose for installing the session replay code was to increase Defendants’

profits (Compl. ¶¶ 294, 337, 400, 439; Opp. at 13). But increasing profit margins is not a tortious purpose. Mot. at 9; *see also Rodriguez v. Google LLC*, 2021 WL 2026726, at *6 n.8 (N.D. Cal. May 21, 2021) (no tortious purpose under the federal act where defendant’s “purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money”).

B. Plaintiffs Fail to Allege The Interception of “Contents”.

Plaintiffs do not persuasively argue that they have alleged the interception of any “contents” under the Federal, California, Maryland, Massachusetts, or Pennsylvania acts.

Plaintiffs’ citation to *Saleh v. Nike, Inc.* is inapposite. In *Saleh*, the plaintiff alleged that the software at issue recorded “a video capturing each of Plaintiff’s keystrokes and mouse clicks on the website.” 562 F. Supp. 3d 503, 518 (C.D. Cal. 2021). Plaintiffs here do not allege that any such “video” was recorded by the session replay software. As numerous courts have held, the simple mouse movements, keystrokes, and mouse clicks that are allegedly collected here do not constitute “contents” of a communication. *See, e.g., Cook*, 2023 WL 5529772 at **8-10; *Goldstein v. Costco Wholesale Corp.*, 559 F. Supp. 3d 1318, 1321 (S.D. Fla. 2021); *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1082–83 (C.D. Cal. 2021); *Jacome v. Spirit Airlines, Inc.*, 2021 WL 3087860 at *4 (Fla. Cir. Ct. June 17, 2021); *Cardoso v. Whirlpool Corp.*, 2021 WL 2820822, at *2 (S.D. Fla. July 6, 2021).

Plaintiffs fail to allege the interception of communication “contents” and therefore Counts I, III, VI, VIII, and XIII should be dismissed.

C. Plaintiffs Do Not Allege A Contemporaneous “Interception”.

Plaintiffs do not dispute that a contemporaneous interception is required to state a claim under the Federal, California, and Maryland acts. Instead, Plaintiffs rely on case law that addresses allegations different from those contained in Plaintiffs’ Complaint. Opp. at 17 (citing *Garcia v.*

Yeti Coolers, LLC, 2023 WL 5736006, at *4 (C.D. Cal. Sep. 5, 2023); *Valenzuela v. Nationwide Mut. Ins. Co.*, 2023 WL 5266033, at *5 (C.D. Cal. Aug. 14, 2023); *Hazel v. Prudential Fin., Inc.*, 2023 WL 3933073, at *3 (N.D. Cal. June 9, 2023)). Here, unlike Plaintiffs’ cited case law, Plaintiffs’ own Complaint alleges that data on user interactions was “accumulated” and later sent “in blocks periodically throughout the user’s website session.” Compl. ¶ 68. This alleged transmission is not contemporaneous and, accordingly, Counts I, III, and VI should be dismissed.

D. Session Replay Code is Not a “Device,” But If It Is then It is a Tracking Device.

In response to Defendants’ arguments that session replay code is not a “device” under the Maryland, Massachusetts, and Pennsylvania statutes, and that, if session replay code is a device, it is a “tracking device,” Plaintiffs make contradictory arguments that wiretap statutes need to be read broadly to include “devices” that were not originally contemplated by the wiretap statutes (Opp. at 17–20), but then that the Pennsylvania statute should be construed narrowly to limit “tracking devices” to those types of devices that were initially contemplated by the legislature. Opp. at 22–23. Plaintiffs cannot have it both ways.

As discussed more fully in Defendants’ Motion, a reasoned reading of the statutes and principles embodied in case law interpreting the statutes leads to the conclusion that a snippet of session replay code is not a “device.” (Mot. at 15–18). Plaintiffs’ opposition to that argument relies largely on cases where courts found a smartphone application that mimics the functionality of a traditional recording device, like a tape recorder, to be a “device” under wiretapping statutes. *See, e.g.*, Opp. at 20 (citing *Commonwealth v. Smith*, 136 A.3d 170, 178 (Pa. Super. 2016)). But session replay code is not a smartphone application—or any type of “application.” Instead, as Plaintiffs allege, session replay code is merely “snippets of JavaScript computer code” that Defendants

allegedly embedded on their websites. Compl. ¶ 1. As session replay code is not a “device,” Counts VI, VII, and XIII should be dismissed.

But if the Court interprets the statutory definitions of “devices” broadly enough to include those snippets of code, then it certainly must also be considered a “tracking device” under the Pennsylvania act. Plaintiffs’ Complaint is rife with references to Defendants allegedly using the session replay code to “track” their customers. *See* Compl. ¶¶ 28, 33, 89, 101, 107, 113, 120, 125, 130, 135, 205, 229, 241–43, 447. The *Jacome* and *Goldstein* cases cited by Defendants (Mot. at 20-21) demonstrate that this type of “tracking” lands session replay code within the definition of “tracking device” in the Pennsylvania statute, requiring dismissal of Count XIII.⁷

E. Session Replay Code Falls Within Maryland’s “Telephone Exemption”

Plaintiffs’ argument that session replay code does not fall under the “telephone exemption” of the Maryland act misses the mark. Opp. at 20–22. Plaintiffs argue that, under *Schmerling*, session replay code cannot fall under the exemption because it is like the monitoring system installed in *Schmerling* to “evaluate and improve customer service.” Opp. at 21 (citing *Schmerling v. Injured Workers’ Ins. Fund*, 795 A.2d 715, 717–18 (Md. 2002)). But unlike the system in *Schmerling*, which was used to improve customer service through training of *human* customer service representatives who happened to use the phones, the session replay code used by Defendants is used to enhance the functionality of the communication device itself—Defendants’ websites—by, for example, fixing broken links. Mot. at 19. This, in turn, has “a positive impact on the . . . communications system.” *Schmerling*, 795 A.2d at 726. Because session replay code

⁷ Plaintiffs’ cite the *Moosejaw* case as rejecting the reasoning in *Goldstein* but *Moosejaw* says nothing about whether session replay code—or any other potential device—is a “tracking device.” It merely states, without analysis, that online shoppers “communicate” with online retailers. *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *1 (N.D. Cal. Oct. 23, 2019).

“further[s] the use of or functionally enhance[s] the []communications system,” it falls within the exemption and Count VI should be dismissed.

F. Plaintiffs’ Consent Bars The Wiretap Claims.

Plaintiffs’ response regarding Plaintiffs’ own consent is unpersuasive. Plaintiffs confuse consent under the various wiretap statutes with the formation of a legally binding contract, arguing, at length, that the Privacy Notices are unenforceable browsewrap agreements and citing to cases assessing the existence of a valid arbitration agreement. Opp. at 25–27 (citing, *e.g.*, *James v. Glob. TelLink Corp*, 852 F.3d 262, 265–67 (3d Cir. 2017)). But Plaintiffs do not cite a single case in their Opposition holding that the equivalent of an enforceable arbitration agreement is required for an individual to manifest consent under any of the wiretap statutes at issue here.

To the contrary, consent under wiretap statutes merely requires that “the person being recorded ‘knew or should have known, that the conversation was being recorded’” but proceeded to make the communication. *See Commonwealth v. Byrd*, 235 A.3d 311, 319 (Pa. 2020) (interpreting the Pennsylvania statute); *see also In re Google Inc.*, 2013 WL 5423918 at *12–13 (N.D. Cal. Sept. 26, 2013) (recognizing consent under federal and California acts can be express or implied). As explained in Defendants’ Motion any reasonable person should have known that their interactions with Defendants’ websites could have been recorded both because of Defendants’ Privacy Notices and because that is how the internet works. Mot. at 21–25; *see also Commonwealth v. Proetto*, 771 A.2d 823, 829 (Pa. Super. Ct. 2001), *aff’d*, 837 A.2d 1163 (Pa. 2003).

Plaintiffs’ claim that the Privacy Notices do not adequately disclose session replay also

misses the mark.⁸ Plaintiffs’ Opposition concedes that Defendants’ Privacy Notices disclose Defendants’ collection of “browsing or search history, website interactions, and advertisement interactions” and then the disclosure of that information “to service providers and others, such as advertising and analytics partners; affiliated companies; law enforcement.” Opp. at 27–28. But Plaintiffs complain that the Privacy Notices do not explicitly say that this collection and disclosure is done “in real time.” Opp. at 28. Even setting aside the fact that, as discussed above and in Defendants’ Motion, Plaintiffs do not adequately allege a contemporaneous interception of any data, Plaintiffs also do not explain why the “real time” nature of a disclosure would invalidate the notice provided by the Privacy Notices. At bottom, Plaintiffs allege that Defendants’ use of session replay code caused Plaintiffs’ website interactions to be captured and disclosed to Defendants’ third-party partners. This is the exact behavior disclosed in Defendants’ Privacy Notices.

Counts I, III, VI, VIII, X, and XIII should all be dismissed.

III. Plaintiffs’ Invasion of Privacy Claims Fail

None of Plaintiffs’ arguments opposing dismissal of the invasion of privacy claims is persuasive.

Intentional Intrusion: In support of their contention that Plaintiffs adequately alleged an intentional intrusion, Plaintiffs point to the allegations in their complaint where they repeat their conclusory allegations that Defendants’ alleged actions were intentional. Opp. at 29–30. But no matter how many times Plaintiffs repeat the words “intentional” or “purposeful,” it does not change the fact that Plaintiffs’ Complaint does not allege that Defendants “believe[d], or [were] substantially certain, that [they] lack[ed] the necessary legal or personal permission” to use session

⁸ Plaintiffs also complain about the placement of Defendants’ Privacy Notices on their websites. Opp. at 26. Defendants note that the placement of the links to their Privacy Notices at the bottom of their homepage is standard practice for websites of nearly every kind—including the website for this Court. See <https://www.paed.uscourts.gov/> (last visited Sept. 29, 2023).

replay code.⁹ *O'Donnell v. United States*, 891 F.2d 1079, 1083 (3d Cir. 1989). Moreover, Plaintiffs do not address Defendants' *Kurowski*, which conclusively held that a defendant allowing "third-party source code to collect [] data" is not an intrusion (intentional or otherwise). *Kurowski v. Rush Sys. for Health*, 2023 WL 2349606, at *9 (N.D. Ill. Mar. 3, 2023).

Expectation of Privacy: Plaintiffs' Opposition ignores the directly on point authority from within this District holding that Plaintiffs "do not have a reasonable expectation of privacy over the anonymized data captured by the Session Replay software at issue here." *Massie*, 2022 WL 534468 at *5. Instead, Plaintiffs point to two opinions where courts addressed different types of data than that allegedly collected by session replay code. Opp. at 30–31 (citing *Facebook Tracking*, 956 F.3d at 604 (analyzing reasonable expectation of privacy in "internet browsing histories" that were allegedly "collected from the *seven million websites* that employ Facebook plug-ins"); *Byars v. Goodyear Tire & Rubber Co.*, 2023 WL 1788553 (analyzing reasonable expectation of privacy in written messages sent through a website's chat feature)).

Highly Offensive Intrusion: Plaintiffs similarly fail to establish that any alleged conduct by Defendants constituted a "highly offensive" intrusion into Plaintiffs' privacy interests. Unlike the examples that Plaintiffs point to in the Opposition, Defendants here, as discussed above and in Defendants' Motion, disclosed the use of tracking like that alleged here in their publicly posted Privacy Policies. Thus, nothing about Defendants' use of session replay code is "duplicitous" or "surreptitious" like the activity described in Plaintiffs' cited cases. Opp. at 31. Here, Defendants'

⁹ For this reason, Plaintiffs' allegations that Defendants "had the option to be less intrusive, but chose to take the more intrusive application of the session replay technology" has no bearing on adequately alleging Defendants' intent. As *O'Donnell* makes clear, the question is not whether Defendants could have configured the session replay technology in a different manner, but whether Defendants were substantially certain that they lacked the necessary legal or personal permission to deploy the session replay technology in the way that they did. *O'Donnell*, 891 F.2d at 1083. Given Defendants' public disclosure of their practices, this is clearly not the case.

use of session replay code was both disclosed to the public and served a legitimate business purpose and accordingly is not the type of “highly offensive” intrusion that can give rise to an invasion of privacy claim. *In re Nickelodeon Cons. Priv. Litig.*, 827 F.3d 262, 294–95 (3d Cir. 2016) (concluding Google’s use of cookies served a legitimate business purpose and was not highly offensive); *Cook*, 2023 WL 5529772 at *10 (“the collection and disclosure of a website visitor’s activity does not constitute the highly objectionable conduct needed to state a claim” for invasion of privacy).

Counts VII, IX, XII, and XIV should be dismissed.

IV. Plaintiffs’ CFAA Claim Fails.

In response to Defendants’ argument that Plaintiffs do not allege Defendants “accessed” Plaintiffs’ computers or mobile devices, Plaintiffs assert that the CFAA allows for conspiracy liability, then state the Complaint alleges “Defendants conspired with SRPs to allow them to access Plaintiffs’ computers and place SRC without consent.” Opp. at 32. But none of the paragraphs Plaintiffs cite alleges, even in a conclusory fashion, that Defendants (or SRPs) ever “access[ed] a computer” or “particular areas of the computer—such as files, folders, or databases—that are off limits to [them].” *Van Buren v. United States*, 141 S. Ct. 1648, 1662 (2021). To the contrary, the allegations relate to the implementation of session replay code *on Defendants’ websites*. See, e.g., Compl. ¶ 146 (discussing “Session Replay Code embedded on [Defendants’] website[s]”).

Next, Plaintiffs mischaracterize Defendants’ argument on “damage” under the statute. As discussed in Defendants’ Motion, and as supported by the numerous cases therein, “damage” under the CFAA must be an impairment *to a computer or computer system*.” *Eagle v. Morgan*, 2011 WL 6739448, at *8 (E.D. Pa. Dec. 22, 2011). Plaintiffs’ cases do not contradict this requirement. See *United States v Soybel*, 13 F.4th 584, 594-95 (7th Cir. 2021) (allowing CFAA claim where injection of code caused user’s password to change, preventing use of the computer); *Bowen v.*

Porsche Cars, N.A., Inc., 561 F. Supp. 3d 1362, 1369–73 (N.D. Ga. 2021) (allowing CFAA claim to proceed where software updates sent to vehicle computers caused the vehicles to not function correctly). Here, Plaintiffs concede that their CFAA claim is premised on “impair[ment to] the value (integrity) of their private information”—not their devices. Opp. at 33. Count II should be dismissed.

V. Plaintiffs’ Unfair Competition Claims Fail.

UCL: Plaintiffs’ claim under California’s unfair competition law fails, first, because Plaintiffs lack statutory standing to pursue the claim. Plaintiffs’ Opposition cites to the *Calhoun v. Google LLC* case, 526 F. Supp. 3d 605 (N.D. Cal. 2021), to say that the alleged interception of Plaintiffs’ personal data satisfies the statutory standing requirement. Opp. at 34. But courts routinely reject this argument. Mot. at 33 (citing *Gardiner v. Walmart Inc.*, 2021 WL 2520103, at *8 (N.D. Cal. Mar. 5, 2021); *Rodriguez*, 2021 WL 2026726, at *8; *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014)); *see also Katz-Lacabe v. Oracle Am., Inc.*, 2023 WL 2838118, at *8 (N.D. Cal. Apr. 6, 2023) (noting the *Calhoun* case and stating that “[t]he weight of the authority in the district and the state, however, point in the opposite direction: that the mere misappropriation of personal information does not establish compensable damages”) (internal quotes omitted). Moreover, even if the diminution of value theory could support UCL standing, Plaintiffs do not address the fact that they do not plausibly allege such damages because they “d[o] not allege they ever attempted or intended to participate in [a] market [for their information], or otherwise to derive economic value from their” data. *Moore v. Centrelake Med. Grp., Inc.*, 299 Cal. Rptr. 3d 544, 564 (Cal. Ct. App. 2022). Count V should be dismissed.

MMPA: Plaintiffs fail to overcome the requirement that the MMPA only applies to individuals who make a “purchase.” The court in *Freeman Health System v. Wass*, as Plaintiffs note (Opp. at 36), affirmed dismissal of an MMPA claim where the individual “paid nothing.”

124 S.W.3d 504, 508 (Mo. Ct. App. 2004). Here, Plaintiff Tucker does not allege that he made any purchase on Defendants’ website. *See* Compl. ¶¶ 127–131. As Plaintiff Tucker does not allege a purchase of merchandise, he cannot state a claim under the MMPA.¹⁰

Additionally, with regard to Plaintiff Tucker’s failure to allege an “ascertainable loss,” Plaintiffs merely repeat the purely speculative assertion that Plaintiff Tucker’s personal information diminished in value and assert that damages should be determined by a jury. *Opp.* at 36. Plaintiffs do not address Defendants’ authority that demonstrates that MMPA cases are properly dismissed where, as here, an “ascertainable loss” is not properly alleged. *Mot.* at 36–37 (citing *Anderson v Bass Pro Outdoor World, LLC*, 355 F. Supp. 3d 830, 837 (W.D. Mo. 2018); *Cregan v. Mortg. One Corp.*, 2016 WL 3072395, at *4 (E.D. Mo. June 1, 2016)). Count XI should be dismissed.

VI. Plaintiffs’ Conversion, Trespass, and Larceny Claims Fail

Conversion and Trespass: Plaintiffs’ Opposition does not mention, much less distinguish, Defendants’ authority showing that the “intermeddling” necessary to state a viable claim for trespass or conversion to chattel requires a physical interference. *Mot.* at 38 (citing, *e.g.*, *Rosemont Taxicab Co. v. Philadelphia Parking Auth.*, 327 F. Supp. 3d 803, 828 (E.D. Pa. 2018)). Accordingly, Plaintiffs’ contentions and cases saying that, as a general proposition, personal property can be intangible, do not save Plaintiffs’ conversion or trespass claims.¹¹ *Opp.* at 37–38. Counts XV and XVI should be dismissed for the reasons set forth in Defendants’ Motion.

¹⁰ Plaintiffs also ignore entirely Defendants’ argument that Plaintiff Tucker fails to allege a causal connection between the supposed fraud and a purchase of merchandise (*Mot.* at 35–36). The MMPA claim should be dismissed on that basis as well.

¹¹ In any event, none of Plaintiffs’ cases stands for the proposition that personal data can be a chattel that forms the basis of a trespass or conversion claim. *See Weicht v. Suburban Newspapers of Greater St. Louis, Inc.*, 32 S.W.3d 592 (Mo. App. 2000) (affirming dismissal of a conversion claim based on intangible property in the form of newspaper routes); *Norris v. Norris*, 731 S.W.2d 844, 845 (Mo. 1987) (construing “intangible personal property” in the context of a will as

Statutory Larceny: The cases that Plaintiffs cite to support their proposition that “copying” of Plaintiffs’ personal data and information constitutes theft do nothing of the kind. As Plaintiffs concede, those cases have found that copying things such as customer lists, files, telephone directories, or trade secrets, can, in some circumstances, be subject to theft through copying. Opp. at 39. Plaintiffs do not explain how their “personal data” is similar to any of these items.

Next, Plaintiffs’ do not dispute that their statutory larceny claim is subject to the heightened pleading requirements of Fed. R. Civ. P. 9(b). Opp. at 39–40. Instead, they list several cases that discuss the elements needed to state a claim for “larceny by trick.” Opp. at 40. But Plaintiffs do not point to any allegations that plead those elements with the requisite particularity. As Defendants argue in their Motion, for the statutory larceny claim to survive, Plaintiffs must allege “facts constituting ‘who, what, when, where, and how of the misconduct alleged.’” Mot. at 40 (citing *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1124 (9th Cir. 2009)). Plaintiffs’ failure to do so dooms their larceny claim.

Finally, Plaintiffs do not appear to respond to Defendants’ argument that Plaintiffs have failed to allege the requisite intent by Defendants, or the cases Defendants cite on that point. Mot. at 40. This lack of alleged intent independently dooms Plaintiffs’ larceny claim.

Count IV should be dismissed.

CONCLUSION

For these reasons, and those contained in Defendants’ Motion, Plaintiffs’ Complaint should be dismissed in its entirety.

“personal property [that] has no intrinsic and marketable value, but is merely the representative or evidence of value, such as certificates of stock, bonds, promissory notes, and franchises”).

September 29, 2023

Respectfully Submitted,

By: /s/ Jennifer A. McLoone
Erin (Loucks) Leffler (PA ID No. 204507)
Shook, Hardy & Bacon L.L.P.
Two Commerce Square
2001 Market St., Suite 3000
Philadelphia, PA 19103
Phone: (215) 278-2555
Fax: (215) 278-2594
eleffler@shb.com

Jennifer A. McLoone (admitted *pro hac vice*)
Shook, Hardy & Bacon L.L.P.
201 South Biscayne Boulevard
Suite 3200
Miami, FL 33131-4332
Phone: (305) 358-5171
Fax: (305) 358-7470
jmcloone@shb.com

Counsel for Defendants